From: Michael A. Alderete
To: Microsoft ATR
Date: 11/10/01 1:53pm
Subject: U.S. v. Microsoft: Security provisions

From <http://www.msnbc.com/news/655131.asp >

> James rejects these criticisms and says the decision to protect Microsoft's security provisions was "one of those `duh' issues." He continues: "Microsoft has security protocols. Are we going to tell everyone how they work? Do you want people to get access to your credit-card information when you shop on line?"

You obviously don't understand electronic security and encryption. The only security systems that work are those where everyone knows how they work. Depending on keeping the mechanism secret GUARANTEES that the security will eventually be broken. Requiring the mechanism to remain secret means the security system is not very strong.

There's plenty of security systems which are publicly documented and well-understood, and which still stand up to attack. Maybe you've heard of DES, AES, and other current encryption systems.

History is riddled with security systems which were kept secret, and then were broken. Recent examples are CSS for DVDs, various watermarking techniques for digital music, and Microsoft's Passport system. The most famous example is Enigma, the "unbreakable" cipher system used by the Germans in WWII. Have you heard of WWII?

Don't hide your settlement loopholes behind the word "security," because it's a lie, and eventually people will recognize it as a lie, and hang you for it.

--

Michael A. Alderete <mailto:michael@alderete.com>
<http://www.alderete.com>
voice: (415) 861-5758